Notice of Allowability	Application No.	Applicant(s)	
	09/598,777	MCCOWN ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *to the Appeal Brief filed on 08 August 2005*.

2. ☒ The allowed claim(s) is/are *1,3-6,13,15-18,24,26-29,31,32,34-37,39 and 41-45*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Status of Claims

1. This action is in response to the Appeal Brief filed on 08 August 2005.

2. Claims 2, 7-12, 14, 19-23, 25, 30, 33, 38, and 40 have been cancelled in the Examiner's amendment shown below.

3. Claims 1, 13, 18, 24, 32, 37, and 39 have been amended in the Examiner's amendment shown below.

4. Claims 41-45 have been added in the Examiner's amendment shown below.

5. Claims 1, 3-6, 13, 15-18, 24, 26-29, 31, 32, 34-37, 39, and 41-45 are currently pending and have been examined.

Allowable Subject Matter

6. Claims 1, 3-6, 13, 15-18, 24, 26-29, 31, 32, 34-37, 39, and 41-45 are allowed. See Reasons for Allowance under separate heading.

Information Disclosure Statement

7. The Information Disclosure Statement filed has been considered. An initialed copy of the Form 1449 is enclosed herewith.

EXAMINER'S AMENDMENT

8. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

9. Authorization for this examiner's amendment was given in a telephone interview with Wayne Bailey on 07 October 2005.

10. The application has been amended as follows:

CLAIM 1. (CURRENTLY AMENDED) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving prior to the transaction a secret master key from a third party, wherein the master key remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key;

receiving a request for a digest from a requestor;

retrieving the master key;

retrieving unique client information;

the client information being associated with the master key;

creating the digest by hashing the unique client information and the master key;

returning the digest and the unique client information to the requester, wherein the digest and the unique client information will be used for transacting with the third party;

wherein the request further comprises unique requester information and creating the digest further comprises hashing the unique requester information; and

wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the unique requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

CLAIM 2. (CANCELLED)

CLAIM 3. (ORIGINAL) The method recited in claim 1 above, wherein the request includes unique merchant information which is used to access the master key.

CLAIM 4. (ORIGINAL) The method. recited in claim 1 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

CLAIM 5. (ORIGINAL) The method recited in claim 1 above, wherein creating the digest by hashing is performed by a smart card.

CLAIM 6. (ORIGINAL) The method recited in claim 1 above further comprises encrypting the unique client information prior to retrieving the unique client information.

CLAIM 7. (CANCELLED)

CLAIM 8. (CANCELLED)

CLAIM 9. (CANCELLED)

CLAIM 10. (CANCELLED)

CLAIM 11. (CANCELLED)

CLAIM 12. (CANCELLED)

CLAIM 13. (CURRENTLY AMENDED) A method for securing a transaction in order to prevent fraudulent transactions, said method comprising:

receiving, prior to the transaction, a secret master key from a third party, wherein the master key remains unchanged, and is not altered after the transaction, the third party storing a copy of the master key within the third party, the master key being kept secret;

receiving, by the third party, a transaction request from a requestor, wherein the transaction request includes a digest and unique client information, the unique client information being associated with the master key;

accessing the copy of the master key based on the unique client information;

creating an authorization digest by hashing the unique client information and the copy of the master key;

comparing, by the third party, the authorization digest with the digest from the requestor;

returning a response to the requester from the third party, the content of the response being based on an outcome of the comparison of the authorization digest with the digest from the requestor;

wherein the request includes unique requestor information and creating the authorization digest further comprises hashing the unique requestor information; and

wherein the third party is a credit card issuer, the transaction is a credit card transaction and the requester is a merchant, further wherein the requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

CLAIM 14. (CANCELLED)

CLAIM 15. (ORIGINAL) The method recited in claim 13 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

CLAIM 16. (ORIGINAL) The method recited in claim 15 above further comprises:

accessing all previously used reference numbers associated with the unique client information;

comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning a response to the requestor, the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

CLAIM 17. (ORIGINAL) The method recited in claim 13 above, wherein creating the authentication digest by hashing is performed by a smart card.

CLAIM 18. (CURRENTLY AMENDED) The method recited in claim 13 above further comprises decrypting the unique client information prior accessing the copy of the master key.

CLAIM 19. (CANCELLED)

CLAIM 20. (CANCELLED)

CLAIM 21. (CANCELLED)

CLAIM 22. (CANCELLED)

CLAIM 23. (CANCELLED)

CLAIM 24. (CURRENTLY AMENDED) A system for securing a transaction in order to prevent fraudulent transactions comprising:

receiving means for receiving a secret master key from a third partition prior to the transaction, the master key remaining unchanged after the transaction, the master key being kept secret;

receiving means for receiving a request for a digest from a requester;

retrieving means for retrieving the master key;

retrieving means for retrieving unique client information;

the client information being associated with the master key;

creating means for creating the digest by hashing the unique client information and the master key;

returning means for returning the digest and the unique client information to the requester, wherein the digest and the unique client information will be used for transacting with the third party;

wherein the request further comprises unique requester information and creating the digest further comprises hashing the unique requestor information; and

wherein the transaction is a credit card transaction, the third party is a credit card issuer, and the requestor is a merchant, further wherein the unique requester information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

CLAIM 25. (CANCELLED)

Claim 26. (ORIGINAL) The system recited in claim 24 above, wherein the request includes unique merchant information which is used to access the master key.

Claim 27. (ORIGINAL) The system recited in claim 24 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

Claim 28. (ORIGINAL) The system recited in claim 24 above, wherein the creating means for creating the digest by bashing is performed by a smart card.

Claim 29. (ORIGINAL) The system recited in claim 24 above farther comprises encrypting means for encrypting the unique client information prior to returning the unique client information.

CLAIM 30. (CANCELLED)

Claim 31. (ORIGINAL) The system recited in claim 24 above further comprises:

fingerprint reading and identification means for reading a fingerprint and authorizing a client based on an identity of a client's fingerprint.

CLAIM 32. (CURRENTLY AMENDED) A system for securing a transaction in order to prevent fraudulent transactions comprising:

providing means for providing from a third party a secret master key to a client, the master key remaining unchanged after the transaction;

receiving means for receiving a transaction request from a requestor, wherein the transaction request includes a digest and unique client information, the digest being created utilizing the master key provided to the client and the unique client information, the unique client information being associated with the master key;

accessing means for accessing, by the third party, a master key stored within the third party based on the unique client information;

creating means for creating an authorization digest by hashing the unique client information

and the master key;

comparing means for comparing the authorization digest with the digest from the requester;

returning means for returning a response to the requestor, the content of the response being based on the outcome of the comparison of the authorization digest with the digest from the requestor;

wherein the request includes unique requester information and creating the authorization digest further comprises hashing the unique requester information; and

wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requester is a merchant, further wherein the requester information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

CLAIM 33. (CANCELLED)

CLAIM 34. (ORIGINAL) The system recited in claim 32 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

CLAIM 35. (ORIGINAL) The system recited in claim 34 above further, comprises:

accessing means for accessing all previously used reference numbers associated with the unique client information;

comparing means for comparing the previously used reference numbers with the reference number contained in the unique client information; and

returning means for returning a response to the requester., the content of the response being based on the outcome of the comparison of the previously used reference numbers with the reference number contained in the unique client information.

CLAIM 36. (ORIGINAL) The system recited in claim 32 above, wherein creating the authentication digest by hashing is performed by a smart card.

CLAIM 37. (CURRENTLY AMENDED) The system recited in claim 32 above further comprises decrypting the unique client information prior accessing the copy of the master key.

CLAIM 38. (CANCELLED)

CLAIM 39. (CURRENTLY AMENDED) A computer program product for securing a transaction in order to prevent fraudulent transactions embodied on a computer readable medium comprising:

providing instructions for providing from a third party a secret master key, the master key remaining unchanged after the transaction;

receiving instructions for receiving a request for a digest from a requester;

retrieving instructions for retrieving the master key;

retrieving instructions for retrieving unique client information;

the master key being associated with the client information;

creating instructions for creating the digest by hashing the unique client information and the master key;

returning instructions for returning the digest and the unique client information to the requestor, wherein the digest and the unique client information will be used for transacting with the third party.

wherein the request includes unique requester information and creating the authorization digest further comprises hashing the unique requester information; and

wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requester is a merchant, further wherein the requester information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier

which is specific to the credit card issuer and transaction data which is specific to a transaction initiated by the client.

CLAIM 40. (CANCELLED)

CLAIM 41. (NEW) The method recited in claim 39 above, wherein the request includes unique merchant information which is used to access the master key.

CLAIM 42. (NEW) The method recited in claim 39 above, wherein the unique client information includes a reference number, the reference number being one of a plurality of reference numbers provided to the client by the third party.

CLAIM 43. (NEW) The method recited in claim 39 above, wherein creating the digest by hashing is performed by a smart card.

CLAIM 44. (NEW) The method recited in claim 39 above further comprises encrypting the unique client information prior to retrieving the unique client information.

Claim 45. (NEW) The system recited in claim 39 above further comprises:

fingerprint reading and identification means for reading a fingerprint and authorizing a client based on an identity of a client's fingerprint.

Reasons For Allowance

11. The following is an Examiner's statement of reasons for allowance:

None of the art of record, taken individually or combination, disclose at least the method step or system components of:

- *receiving prior to the transaction a secret master key from a third party, wherein the master key remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key;*
- *creating the digest by hashing the unique client information and the master key;*
- *returning the digest and the unique client information to the requester, wherein the digest and the unique client information will be used for transacting with the third party;*
- *wherein the request further comprises unique requester information and creating the digest further comprises hashing the unique requester information; and*
- *wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the unique requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.*

More specifically, the prior art of record fails to disclose creating a message digest by hashing the master key with the unique client information, unique requestor information that contains information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.

Independent Claims 1, 13, 24, 32, and 39 are distinguished over the closest prior art of Muftic which teaches that when using hashes, the method for determining if a message is authentic is by doing a similar hash and comparing the results (C2, L27-37). Moreover,

Muftic clearly teaches that the way to authenticate a hashed message is by using the same components, doing a parallel hash, and comparing the results. As recited in the independent claims, it is clear that the Applicant's invention is distinguished over the Muftic invention in at least the method steps and system components of:

- *receiving prior to the transaction a secret master key from a third party, wherein the master key remains unchanged and is kept secret, and is not altered after the transaction, the third party storing a copy of the master key;*
- *creating the digest by hashing the unique client information and the master key;*
- *returning the digest and the unique client information to the requester, wherein the digest and the unique client information will be used for transacting with the third party;*
- *wherein the request further comprises unique requester information and creating the digest further comprises hashing the unique requester information; and*
- *wherein the transaction is a credit card transaction, the third party is a credit card issuer and the requestor is a merchant, further wherein the unique requestor information includes information describing a merchant identifier which is specific to the credit card issuer, a transaction identifier which is specific to the credit card issuer and purchase information which is specific to a purchase initiated by the client.*

Although Muftic does disclose hashing and public key infrastructure, Muftic does not specifically disclose a master key *per se*, hashing a master key with customer information, and the inherent transactional steps associated with a smart card transaction.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James Trammell** can be reached at **571.272.6712.**

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

571-273-8300 [Official communications, After Final communications labeled "Box AF"]

571-273-8300 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

13 October 2005